# DNS Zone Transfer Attack

Sometimes DNS servers are misconfigured. The DNS server contains a Zone file which it uses to replicate the map of a domain. They should be configured so that only the replicating DNS-server can access it, but sometimes it is misconfigured so anyone can request the zone file, and thereby recieve the whole list of subdomains. This can be done the following way:

To do this we first need to figure out which DNS-servers a domain has.

```
host -t ns wikipedia.com
```

```
host -l wikipedia.com ns1.wikipedia.com
```

This can also be done with tools such as dnsrecon and dnsenum.

https://security.stackexchange.com/questions/10452/dns-zone-transfer-attack